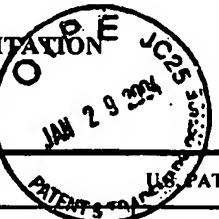
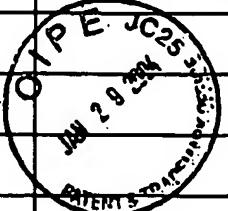
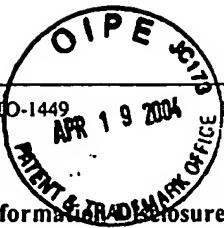


INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary).</i>				Docket Number (Optional) 43521-0700		Application Number 10/622,722	
				Applicant(s) Hidema TANAKA, Toshinobu KANEKO			
				Filing Date July 18, 2003		Group Art Unit TBA	
U.S. PATENT DOCUMENTS							
*EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
FOREIGN PATENT DOCUMENTS							
REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Translation	
						YES	NO
OTHER DOCUMENTS <i>(Including Author, Title, Date, Pertinent Pages, Etc.)</i>							
CO		Jakobsen & Knudsen "The Interpolation Attack on Block Cipher," FSE-4th International Workshop LNCS 1008					
CO		Nyberg, Knudsen, "Provable Security Against Differential Cryptanalysis," Journal of Cryptology, Vol. 8-no. 1					
EXAMINER /Chinwendu Okoronkwo/				DATE CONSIDERED 01/06/2007			
EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP Section 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.							

INFORMATION DISCLOSURE CITATION <i>(Use several sheets if necessary)</i>				Docket Number (Optional) 43521-0700	Application Number 10/622,722																										
				Applicant(s) Hidema TANAKA, Toshinobu KANEKO																											
				Filing Date July 18, 2003	Group Art Unit TBA																										
				U.S. PATENT DOCUMENTS																											
EXAMINER INITIAL	REF	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE																								
																															
FOREIGN PATENT DOCUMENTS																															
REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Translation																									
						YES	NO																								
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2"></td> <td colspan="6" style="text-align: center;">OTHER DOCUMENTS <i>(Including Author, Title, Date, Pertinent Pages, Etc.)</i></td> </tr> <tr> <td>CO</td> <td></td> <td colspan="6">Shimoyama, Moriai, Kaneko, "Improving the Higher Order Differential Attack and Cryptanalysis of the KN Cipher," 1997 1st International Workshop on Information Security Workshop LNCS 1396, Tatsunokuchi, Ishikawa, Japan, September 1997 (pp 32-42)</td> </tr> <tr> <td>CO</td> <td></td> <td colspan="6">Tanaka, Hisamatsu, Kaneko, "Strength of MISTY1 without FL Function for Higher Order Differential Attack," 13th International (Symposium, Applied Algebra-Algebraic Algorithms and Error-Correcting Codes) 1999, LNCS 1636 (pp 221-231)</td> </tr> </table>										OTHER DOCUMENTS <i>(Including Author, Title, Date, Pertinent Pages, Etc.)</i>						CO		Shimoyama, Moriai, Kaneko, "Improving the Higher Order Differential Attack and Cryptanalysis of the KN Cipher," 1997 1st International Workshop on Information Security Workshop LNCS 1396, Tatsunokuchi, Ishikawa, Japan, September 1997 (pp 32-42)						CO		Tanaka, Hisamatsu, Kaneko, "Strength of MISTY1 without FL Function for Higher Order Differential Attack," 13th International (Symposium, Applied Algebra-Algebraic Algorithms and Error-Correcting Codes) 1999, LNCS 1636 (pp 221-231)					
		OTHER DOCUMENTS <i>(Including Author, Title, Date, Pertinent Pages, Etc.)</i>																													
CO		Shimoyama, Moriai, Kaneko, "Improving the Higher Order Differential Attack and Cryptanalysis of the KN Cipher," 1997 1st International Workshop on Information Security Workshop LNCS 1396, Tatsunokuchi, Ishikawa, Japan, September 1997 (pp 32-42)																													
CO		Tanaka, Hisamatsu, Kaneko, "Strength of MISTY1 without FL Function for Higher Order Differential Attack," 13th International (Symposium, Applied Algebra-Algebraic Algorithms and Error-Correcting Codes) 1999, LNCS 1636 (pp 221-231)																													
EXAMINER /Chinwendu Okoronkwo/			DATE CONSIDERED 01/06/2007																												
EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP Section 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.																															



Sheet 1 of 1

Substitute Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney's Docket No. 43521-0700	Application No. 10/622,722
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Tanaka et al.	Filing Date July 18, 2003
		Group Art Unit TBD	

U.S. Patent Documents

Foreign Patent Documents or Published Foreign Patent Applications

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
CO		L. Knudsen, "Truncated and Higher Order Differentials," <i>Fast Software Encryption: 2nd International Workshop</i> , Leuven, Belgium (December 14-16, 1994), LNCS 1008, pp. 196-211, Springer-Verlag.
CO		X. Lai, "Higher Order Derivatives and Differentia Cryptanalysis," R ³ Security Engineering AG Ch-8607 Aathal, Switzerland, pp. 1-7; Reprint of pp. 227-233, "Communications and Cryptography," (Ed. R Blahut et al.), Kluwer Academic Publishers (1994).
CO		M. Matsui, "New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis, <i>Fast Software Encryption: 3rd International Workshop</i> , Cambridge, UK (February 21-23, 1996), LNCS. 1039, pp. 205-218.
CO		S. Moriai, T. Shimoyama, T. Kaneko, "Higher Order Differential Attack of a CAST Cipher, <i>Fast Software Encryption: 4th International Workshop</i> , LNCS 1372, pp. 17-31.

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.